NOREA Taskforce DORA

Topic: Overview of all DORA legislation including current status per standard
From: NOREA Taskforce DORA
Date: July 2nd 2025
Authors: Jesper de Boer & Sandeep Gangaram Panday from the DORA Taskforce

For the full member list and more content created by the Taskforce, please see https://www.norea.nl/dora

Introduction DORA

In light of the evolving and increasing dependencies on ICT systems, the EU introduced DORA to address multifaceted risks within the financial sector. Officially known as Regulation (EU) 2022/2554, DORA is a legislative act intended to ensure that financial entities within the EU can withstand, respond to, and recover from all types of ICT-related disruptions and threats.

DORA level 1

DORA lays out several key requirements, referred to as level 1 regulations, to achieve its objectives. Described in the act itself, these requirements are discussed in the context of DORA's five foundational pillars:

1. ICT risk management;
2. Incident management, classification, and reporting;
3. Digital operational resilience testing;
4. Management of ICT third-party risks;
5. Information-sharing arrangements.

The DORA regulation was published on December 27, 2022: Regulation- 2022/2554- EN- DORA- EUR-Lex

DORA level 2

The main text of DORA is supplemented by important technical detail in a body of secondary legislation, referred to as level 2 regulations. The three European supervisory authorities (ESAs) were jointly appointed to draft these standards. The ESAs consist of the European Banking Authority (EBA), the European Insurance and Occupational Pensions Authority (EIOPA), and the European Securities and Markets Authority (ESMA).

These technical standards consist of two types:

- Regulatory technical standards (RTS), of which there are seven;
- Implementation technical standards (ITS), of which there are two.

Development of the RTS and ITS was separated into work on two sets of documents. The first set was submitted to the European Commission (EC) on 17 January 2024. The three RTS documents in this first set were published in the *Official Journal of the European Union* on 25 June 2024, signaling their official adoption.

The first set consists of the following documents:

- RTS on ICT risk management framework including the simplified ICT risk management framework article 28-41 (part of DORA's first pillar);
- RTS on criteria for the classification of ICT-related incidents (second pillar);
- ITS to establish the templates for the register of information (fourth pillar);
- RTS to specify the policy on ICT services performed by ICT third-party providers (fourth pillar).

The second set, which was submitted to the EC in two parts, on 17 July 2024 and 26 July 2024, consists of the following documents:

- RTS on content, timelines, and templates on incident reporting (part of DORA's second pillar);
- ITS on content, timelines, and templates on incident reporting (second pillar);
- RTS on subcontracting of critical or important functions (fourth pillar);
- RTS on oversight harmonization (fourth pillar);
- RTS on threat-led penetration testing TLPT (third pillar).

Current status of DORA level 2 legislation

Since December 2022, the publication of DORA, a lot of requirements have been published, adjusted and republished. From draft publications to final publications in the EU-journal. Not all requirements were initially accepted by the European Commission. It can be quite challenging to keep up with all the requirements. Currently, there is no overview available providing the current status of all DORA level 2 documents.

In table 1 below we provide an overview of the current level 2 documents and links to latest versions. As can be concluded, all of all level 2 documents are final.

NOREA Taskforce DORA

Pillar	Short name	ITS / RTS / Guideline	Status July 2, 2025	Link to current version	Latest update
1. ICT Risk-management	Normal and simplified ICT Risk-management	RTS	EU Journal	Delegated regulation- EU- 2024/1774- EN- EUR-Lex	June 2024
2. Incidents	Time limits reporting	RTS	EU Journal	Delegated regulation- EU- 2025/301- EN- EUR-Lex	February 2025
2. Incidents	Criteria classification on incidents	RTS	EU Journal	Delegated regulation- EU- 2024/1772- EN- EUR-Lex	June 2024
2. Incidents	Major incident Reporting (templates)	ITS	EU Journal	Implementing regulation- EU- 2025/302- EN- EUR-Lex	February 2025
2. Incidents	Cost and losses incidents	Guideline	Final publication	Joint Guidelines on estimation of aggregated annual costs and losses caused by major ICT-related incidents | European Banking Authority	June 2025
3. Resilience	Threat-led penetration testing	RTS	EU Journal	Delegated regulation- EU- 2025/1190- EN- EUR-Lex	June 2025
4. Third party	Contractual arrangements on the use of ICT services supporting critical or important functions	RTS	EU Journal	Delegated regulation- EU- 2024/1773- EN- EUR-Lex	June 2024
4. Third party	Subcontracting	RTS	EU Journal	Delegated regulation- EU- 2025/532- EN- EUR-Lex	July 2025
4. Third party	Register of information	ITS	EU Journal	Implementing regulation- EU- 2024/2956- EN- EUR-Lex	December 2024
Other	Oversight harmonization	RTS	EU Journal	Delegated regulation- EU- 2025/295- EN- EUR-Lex	February 2025
Other	Oversight cooperation and information exchange between the ESA	Guideline	Final publication	Joint Guidelines on the oversight cooperation and information exchange between the ESAs and the competent authorities | European Banking Authority	June 2025

Table 1: DORA Level 2 status update on July 2nd 2025

Appendix A: Other interesting updates and links

For the Dutch Financial Institutions

In the Netherlands, the main requirements for financial institutions are documented in the Wet op het Financieel Toezicht. Due to DORA, some changes to the "Wet op het Financieel Toezicht" have been made and are published in June and November 2024:

- stb-2024-199.pdf (enforcing DORA in Dutch law)
- stb-2024-379.pdf (elaborating on the fines and publication of fines)

The Wft now includes an appendix with classifies fines for non-compliance: wetten.nl- Regeling- Besluit EU-verordeningen Wft- BWBR0049497

Third parties and Register of Information (ROI)

During summer 2024 a dry run for ROI was performed by a large number of financial institutions. The dry run results, with a focus on Data quality:

- ESA_2024_35_DORA_Dry_Run_exercise_summary_report.pdf

For the latest FAQ and templates for ROI:

- Preparations for reporting of DORA registers of information | European Banking Authority

The Institute of International Finance published a staff paper, "Third-Party Risk Management and Operational Resilience in Financial Services:

- Third-Party Risk Management & Operational Resilience in Financial Services > The Institute of International Finance

The SMA has published the priciples of third party risk supervision:

- https://www.esma.europa.eu/sites/default/files/2025-06/ESMA42-1710566791-6103_Principles_on_third-party_risks.pdf

Incidents

ESAS published a report on the feasibility for further centralisation of reporting of major ICT-related incidents. This gives insight in why it's important to timely report:

- https://www.eiopa.europa.eu/document/download/47b6ad86-3a4b-4d00-9acd-088ef9e64d18_en?filename=JC%202024%20108_Report%20on%20the%20feasibility%20for%20further%20Centralisation%20of%20reporting%20of%20major%20ICT%20incidents.pdf

Resilience

For inspiration of the threat landscape for resilience testing (article 24 DORA):

- ENISA Threat landscape: Finance sector

ISACA published a White Paper regarding Resilience and Security with relation to NIS2 and DORA:

- White Papers 2025 Resilience and Security in Critical Sectors Navigating NIS2 and DORA Requirements

The ECB published the Tiber-framework:

- What is TIBER-EU?

Other relevant publications

- The official Q&A on DORA: Q&A on regulation- EIOPA
- ESA's: Point of view of non-existence transition period: Microsoft Word- JC 2024 99_Statement start DORA application_final clean
- AFM: Checklist and periodic update publications: Digital Operational Resilience Act (DORA)
- DNB: Good Practice 2023: Q&A Informatiebeveiliging | De Nederlandsche Bank
- DNB: Oversight 2025: DORA: het toezicht van DNB per 17 januari 2025 | De Nederlandsche Bank
- Cyber Security Raad published the Cybersecurity Guidelines for Directors and Business Owners (Dutch only): Handreiking Cybersecurity voor Bestuurders en Bedrijfseigenaren | Cyber Security Raad
- NOREA: For amongst other DORA Control Framework, template Exit plan and incident classification tool and Guideline boardroom training: NOREA | Digital Operational Resilience Act- DORA

Disclaimer

All links are validated on July 2, 2025. We are not responsible for any errors or omissions in this content or any damages resulting from its use.

This article is a follow up on our previous overview with in depth analyses of changes, in Dutch only: Analyse wijzigingen 2e batch RTS DORA – Juli 2024 | LinkedIn.